



CVE-2014-5018

Published on: 07/21/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:52 PM UTC

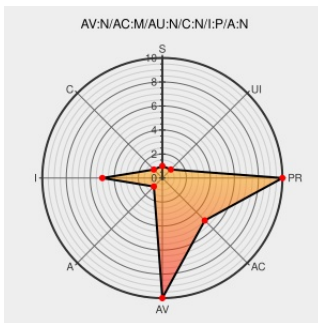
CVE-2014-5018

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Limesurvey](#) from [Limesurvey](#) contain the following vulnerability:

Incomplete blacklist vulnerability in the autoEscape function in common_helper.php in LimeSurvey 2.05+ Build 140618 allows remote attackers to conduct cross-site scripting (XSS) attacks via the GBK charset in the loadname parameter to index.php, related to the survey resume.

CVE-2014-5018 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Fixed issue: Vulnerable parameter on survey resume - LimeSurvey/LimeSurvey@3a6dd6b - GitHub

[Exploit](#)
[Patch](#)
[github.com](#)
[text/html](#)

CONFIRM
github.com/LimeSurvey/LimeSurvey/commit/3a6dd6b44cef2fa3f96f403e1cb9

Lime Survey 2.05+ Build 140618 XSS / SQL Injection ≈ Packet Storm

[Exploit](#)
[packetstormsecurity.com](#)
[text/html](#)

MISC packetstormsecurity.com/files/127369/Lime-Survey-2.05-Build-140618-XSS-SQL-Injection.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Limesurvey	Limesurvey	2.05+	All	All	All
Application	Limesurvey	Limesurvey	2.05\+	All	All	All
Application	Limesurvey	Limesurvey	2.05\+	All	All	All
cpe:2.3:a:limesurvey:limesurvey:2.05+:::*:*:*:*:*:						
cpe:2.3:a:limesurvey:limesurvey:2.05\+:::*:*:*:*:*:						
cpe:2.3:a:limesurvey:limesurvey:2.05\+:::*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)